UNIVERSITY OF SUSSEX

General Counsel, Governance and Compliance

INFORMATION CLASSIFICATION AND HANDLING POLICY

1. OVERVIEW AND PURPOSE

1.1 The University needs to safeguard its information and, in relation to information that is personal data, has a duty to comply with the principles and requirements of data protection legislation[1] when processing such data.

1.2 The Information Classification and Handling Policy has been developed to sit alongside the Information Security policies and the Data Protection Policy and is in place to ensure that all information handled[2] by the University – whether personal data or not – is handled with appropriate care and security at all times.

1.3 This policy outlines how information should be categorised based on risk and details the associated required protective measures that must be used when handling different types of information.

1.4 The Information Classification & Handling Policy will ensure that a consistent approach to handling information is employed across the University and will reduce the risk of information breaches.

2. SCOPE

2.1 This policy applies to all information handled – internally or externally – by the University including information created by members of the University or received from third parties. The policy relates to information whether it is held electronically or physically.

2.2 This policy applies to all staff and others handling information, either remunerated or not, including:

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;

[1] Data protection legislation is any applicable legislation relating to the processing of personal data and includes the Data Protection Act 2018, the UK General Data Protection Regulation and, in certain circumstances, the EU General Data Protection Regulation 2016/679.

[2] Handling includes the recording, organisation, storage, use, disclosure, sharing, transmission and destruction of information and any 'processing' of personal data, as defined in data protection legislation.

- Volunteers, apprentices, and interns; and

- Others associated with (i.e. performing services for or on behalf of) the University (including agents, sponsors, contractors, representatives, consultants, and other service providers), or who are otherwise deemed to be covered by this policy by the Chief Operating Officer.

2.3 Except where a student is also an employee of the University, or handling information as a part of the University (e.g. as part of research work), this policy does not apply directly to students.

3. RESPONSIBILITIES

3.1 The University

3.1.1 The University is responsible for ensuring appropriate technical and organisational measures are in place to safeguard any information that is handled as a part of its functions.

3.1.2 The University is responsible for compliance with all legislative and regulatory requirements relating to data protection and information security.

3.2 Information Governance Committee

3.2.1 The Information Governance Committee is responsible for reviewing the operational status of information security, data protection, information risk management, and records management, as well as having oversight of the University's regulatory and legislative obligations with regard to information and data.

3.2.2 The Information Governance Committee has oversight of the University's Information Classification and Handling Policy and is responsible for ensuring resources are made available to meet the requirements of the policy.

3.3 The Senior Information Risk Owner (SIRO)

3.3.1 The SIRO is the named individual responsible for leading a culture of good information management and governance within the University, including the appropriate classification and handling of information.

3.3.2 The SIRO ensures that information assets and risks within the University are managed appropriately and effectively via consistent organisational processes, and that policies and procedures to facilitate this are in place.

3.3.3 The SIRO will delegate responsibility for ensuring compliance with this policy in terms of information technologies used by the University to the Director of IT Services.

3.4 Director of IT Services

3.4.1 The Director of IT Services is responsible for ensuring that information technologies used by the University enable compliance with this policy.

3.5 Heads of Schools and Professional Services Directors

3.5.1 Heads of Schools and Professional Services Directors have responsibility for ensuring that their staff are familiar with this policy and that classification and handling of information throughout the School or Division is in compliance with this policy.

3.6 All Individual Staff Members

3.6.1 All staff are responsible for familiarising themselves with this policy and complying with it.

3.6.2 All staff must ensure that information they handle is appropriately classified and handled in accordance with this policy and the Information Classification and Handling Matrix.

4. POLICY

4.1 Classification of information

4.1.1 All information handled by the University which is confidential or has value (financial or otherwise) must be protected at all times. Information must be classified and the appropriate safeguards and measures put into place to protect the information, based on that classification.

4.1.2 All information in the University must be classified into one of four categories based on a risk assessment of its sensitivity or value, by those who own or are responsible for the information, or handle the information:

- *Public/Open* – the information is legitimately in the public domain or is appropriate for disclosure or dissemination to the public without the need for restrictions or controls.

- *Internal use* – information can be disclosed and shared with appropriate individuals at the University (e.g. staff and students), with minimal restrictions on its internal disclosure, for example, available to authenticated users of Sussex systems, virtual learning environments and lecture capture services.

Information such as video capture of lectures and Committee papers would fall within this classification.

- *Sensitive* – sensitive information requires appropriate controls and measures in place, and needs to be handled in a manner that prevents unauthorised access. Inappropriate disclosure or dissemination would likely cause financial or reputational damage to the University, or impact on individuals. Examples include 'personal data' as defined by data protection legislation (in particular, special categories of personal data), confidential information and information that is commercially sensitive.

- *Protected* – protected information has the most significant value for the University and its unauthorised disclosure or dissemination would result in severe financial or reputational damage to the University, or significant harm to individuals. Access to such information must be explicitly granted and access must be protected by appropriate information security measures. Examples include information relating to security or the prevention or detection of crime, or highly valuable commercial or research information, often bound by contractual or legal obligations.

4.1.3 The assessment of risk and the classification of information should take account of the value of the information (financial or otherwise) and the likelihood and impact of harm to the institution or others should the information be wrongly disclosed, altered or lost.

4.1.4 Most information will fall into the '*Public/Open*' or '*Internal use*' categories but, based on data protection requirements or the protection of University interests, some information will be categorised as '*Sensitive*'. In the event of uncertainty as to the classification of information, the default category and handling method should be '*Sensitive*'. Only very limited information would fall within the '*Protected*' category. Where information falls within more than one category, the higher classification shall be applied.

4.1.5 Examples of information falling within the categories can be found in the Information Classification and Handling Matrix. These are examples and should not be considered an exhaustive list.

4.1.6 Once information has been classified, the classification markings must be clearly visible, whether information is handled in paper or electronic format. There is no requirement to mark '*Public/Open*' information.

4.2 **Handling of Information**

4.2.1 Information must be handled according to its classification, with '*Sensitive*' and '*Protected*' information requiring a much greater degree of security. Technical and

organisational measures should be in place to protect against unauthorised or unlawful disclosure or use of information, and against accidental loss, destruction or damage. Such measures will include access controls and information security and, the more value the information has, the greater the level of security required in any technical and organisational measures. '*Protected*' information will require the most robust security measures and access should be controlled and limited, based on senior management approval.

4.2.2 Information should only be held for as long as is necessary and must be retained and destroyed in accordance with the University's Records Management policy and Master Records Retention Schedule. Information, other than '*Public/Open*' information, must be securely disposed of, for example, through secure shredding, confidential waste disposal and IT supported deletion. All IT equipment which holds information, such as laptops and mobile telephones, must be disposed of in a secure manner by IT Services, in accordance with the IT Asset Management Policy and the Workstation Disposal Policy.

4.2.3 Further guidance on the handling of information can be found in the Information Classification and Handling Matrix.

4.3 **Compliance**

4.3.1 Where there is non-compliance with this policy resulting in a personal data breach, any breach must be reported to the University's Data Protection Officer under the Data Breach Reporting Process.

4.3.2 Where there is deliberate misconduct or behaviour amounting to a wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

5. LEGISLATION

5.1 The Information Commissioner's Office provides a guide to the UK data protection legislation on their website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

5.2 Details of the Data Protection Act 2018 can be found at the following link: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

5.3 Details of the Freedom of Information Act 2000 can be found at the following link: https://www.legislation.gov.uk/ukpga/2000/36/contents

Review / Contacts / References	
Policy title:	Information Classification and Handling Policy
Date approved:	3 October 2018
Approving body:	Information Governance Committee
Last review date:	February 2021
Revision history:	Version 1: October 2018 Version 2: February 2021
Next review date:	February 2022
Related internal policies, procedures, guidance:	Information Classification and Handling Matrix Information Security Policy Records Management Policy Master Records Retention Schedule Data Protection Policy Data Breach Reporting Process IT Asset Management Policy Workstation Disposal Policy
Policy owner:	General Counsel, as Senior Information Risk Owner
Lead contact / author:	Karen Blackman, Information Manager Alexandra Elliott, Head of Information Management and Compliance